Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method of communicating to a server machine a certificate of a user which is sent by a client machine via a security module of a computer system, wherein a first protocol used between the client machine and the server machine is a non-secure stateless protocol, and a second protocol used between the client machine and the security module is a secure stateless protocol, said method comprising:

inserting said certificate unmodified into a cookie header of a request in the first protocol; and

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine using said first protocol;

wherein said certificate has a plurality of separators; and

wherein said cookie header of said request includes a plurality of cookies.

2. (currently amended) A method according to claim 1, further comprising:

removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

3. (previously presented) A method according to claim 1, wherein said inserting step further comprises:

determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine; and creating a new cookie header if said existing cookie header is not present in the request sent by the client machine.

4. (previously presented) A method according to claim 3, further comprising:

adding a specific cookie into the existing or new cookie header; and

assigning a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

5. (cancelled).

6. (currently amended) A security machine which secures exchanges between a client machine and a server machine of a computer system, wherein a first protocol used between the client machine and server machine is a non-secure stateless protocol, and a second protocol implemented between the client machine and said security machine is a secure stateless protocol, said security machine comprising:

an analyzer ~~which enables the transmission of a~~ configured to insert an unmodified certificate ~~inserted~~ into a cookie header of an HTTP or equivalent request, and further configured to transmit to a server said unmodified certificate contained in said cookie header using said first protocol;

wherein said cookie header of said request includes a plurality of cookies.

7. (currently amended) A system comprising:

a client machine;

a server machine; and

a security module;

wherein the client machine and the server machine are configured to communicate using a first protocol, said first protocol comprising a non-secure stateless protocol;

wherein the client machine and the security module are configured to communicate using a second protocol, said second protocol comprising a secure stateless protocol; and

wherein the security module comprises an analyzing program configured to insert an unmodified certificate sent by the client machine into a cookie header of a request in conformance with said non-secure stateless protocol, and wherein the analyzing program is further configured to transmit to a server said unmodified certificate contained in said cookie header using said non-secure stateless protocol, ~~which enables transmission of a certificate sent by the client machine in a cookie header of a request in said stateless protocol, wherein~~ said cookie header of said request including ~~includes~~ a plurality of cookies.

8. (currently amended) A computer readable medium upon which is ~~embodied~~ encoded a sequence of programmable instructions which, when executed by a security module of a computer system, cause the security module to perform operations comprising:

communicating to a server machine a certificate of a user which is sent by a client machine via the security module, wherein a first protocol used between the client machine and the server machine is a non-secure stateless protocol, and wherein a second protocol used between the client machine and the security module is a secure stateless protocol;

inserting said certificate unmodified into a cookie header of a request ~~in~~ conforming to the first protocol; and

transmitting the request, including said cookie header containing said unmodified certificate, from the security module to the server machine using said first protocol;

wherein said certificate has a plurality of separators; and

wherein said cookie header of said request includes a plurality of cookies.

9. (new) The computer-readable medium of claim 8, wherein the instructions further comprise:

removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

10. (new) The computer-readable medium of claim 8, wherein the instructions further comprise:

determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine; and

creating a new cookie header if said existing cookie header is not present in the request sent by the client machine.

11. (new) The computer-readable medium of claim 10, wherein the instructions further comprise:

adding a specific cookie into the existing or new cookie header; and assigning a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

12. (new) The system of claim 7, wherein said analyzing program is further configured to:

remove from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

13. (new) The system of claim 7, wherein said analyzing program is further configured to:

determine, prior to said inserting, whether an existing cookie header is present in the request sent by the client machine; and

create a new cookie header if said existing cookie header is not present in the request sent by the client machine.

14. (new) The system of claim 13, wherein said analyzing program is further configured to:

add a specific cookie into the existing or new cookie header; and

assign a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.

15. (new) The security machine of claim 6, wherein said analyzer is further configured to:

remove from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header of said request.

16. (new) The security machine of claim 6, wherein said analyzer is further configured to:

determine, prior to said inserting, whether an existing cookie header is present in the request sent by the client machine; and

create a new cookie header if said existing cookie header is not present in the request sent by the client machine.

17. (new) The security machine of claim 16, wherein said analyzer is further configured to:

add a specific cookie into the existing or new cookie header; and

assign a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request.